

Inspector General

United States Department of Defense



DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSESSMENTS

Assessment of Security Within the Department of Defense - Security Policy

This document will not be released (in whole or in part) outside the Department of Defense without the prior written approval of the Inspector General of the Department of Defense

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 27 JUL 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Assessment of Security Within the Department of Defense - Security Policy				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense Inspector General, 4800 Mark Center Drive, Alexandria, VA, 22350-1500				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 17	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/Ir/reports.htm> or contact the DoD Office of Inspector General at (703) 882-4818 or (DSN) 381-4818.

Suggestions for Audits and Evaluations

To suggest ideas for or to request future audits or evaluations, contact the Office of the Deputy Inspector General for Intelligence and Special Program Assessments at (703) 882-4860 (DSN 381-4860) or UNCLASSIFIED fax (571) 372-7451. Ideas and requests can also be mailed to:

ODIG-ISPA (ATTN: ISPA Suggestions)
Department of Defense Inspector General
4800 Mark Center Drive (Suite 10J25)
Alexandria, VA 22350-1500



Acronyms and Abbreviations

DSE	Defense Security Enterprise
DSE ExCom	Defense Security Enterprise Executive Committee
DTM	Directive-Type Memorandum
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
SPeD	Security Professional Education and Development
USD(I)	Under Secretary of Defense for Intelligence



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 27, 2012

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DEPUTY UNDER SECRETARY OF DEFENSE FOR
INTELLIGENCE AND SECURITY

SUBJECT: Assessment of Security Within the Department of Defense -
Security Policy (Report No. DoDIG-2012-114)

We are providing this report for your information and use. This is the third in a series of reports designed to provide an overall assessment of security policies and procedures within the Department. No written response to this report was required; however, comments were provided and are included in the Management Comments section.

We appreciate the courtesies extended to the staff. Please direct questions to Mr. William Rainey at (703) 882-4841 (DSN 381-4841), william.rainey@dodig.mil or the Project Manager at (703) 882-4834 (DSN 381-4834).

A handwritten signature in black ink, appearing to read "J. Ives", is positioned above the printed name and title of the signatory.

James R. Ives
Acting Deputy Inspector General
for Intelligence and Special
Program Assessments



Results in Brief: Assessment of Security Within the Department of Defense – Security Policy

What We Did

This is the third in a series of reports designed to provide an overall assessment of security policies and procedures within the Department. In this report, we assessed how effective security policy is in addressing the security needs of the Department. We addressed security costs, and training, certification, and professionalization in previous reports. Classification and grading of security jobs will be the final report in this series.

What We Found

We found that security policies often overlap, are fragmentary, or inconsistent. In addition, the sheer volume of security policies that are not coordinated or integrated makes it difficult for those at the field level to ensure consistent and comprehensive policy implementation. While compliance with existing security policies remains a central issue, consumers at the field level are often required to interpret outdated security policy guidance to make it relevant to existing organizational requirements.

In the first report in this series, Report No. 10-INTEL-09, “Assessment of Security Within the Department of Defense: Tracking and Measuring Security Costs,” August 6, 2010, we recommended a comprehensive and integrated security framework to facilitate tracking security costs, more accurately programming future years security budgets, and examine the return on investment for security expenditures. The Deputy Under Secretary of Defense for Intelligence and Security agreed, stating that an overarching security policy is the necessary first step to provide a platform for functional integration, governance, and strategic resource management.

The Under Secretary of Defense for Intelligence is in the process of promulgating an overarching security policy, “Management of the Department of Defense Security Enterprise,” that provides guidance for a comprehensive and integrated security framework. This action is scheduled to be completed in the fourth quarter of 2012. Also, the Under Secretary of Defense for Intelligence has created the Defense Security Enterprise Executive Committee, a senior-level governance body for the strategic administration and policy coordination of the Defense Security Enterprise.

However, until the overarching security policy is promulgated and the Defense Security Enterprise Executive Committee becomes an inculcated and inclusive governing process, interoperability issues, redundancies, and other inefficiencies will persist.

What We Recommend

We are not making any recommendations in this report because the overarching security policy and the Defense Security Enterprise Executive Committee will ensure an enterprise approach to security policy across the Department. Further, our previous recommendation should ensure that the new Defense Security Enterprise Executive Committee will be an integral part of policy development and coordination with the requisite authorities to effect changes in security policy implementation and oversight.

Management Comments

Although not required, the Deputy Under Secretary of Defense for Intelligence and Security provided comments in response to this report.

Table of Contents

Introduction	1
Objectives	1
Scope and Methodology	1
Background	2
Finding. DoD Needs an Overarching Security Policy to Advance an Integrated Enterprise Approach to Security	3
Appendix: Prior Coverage	10
Management Comments	11

Introduction

Security spans the entire Department and is necessary for the Department to protect its resources. Department of Defense security disciplines have as one fundamental purpose the protection of DoD critical assets and must be applied in a fully balanced and coordinated way. Actions taken in one area, for example, physical security, have a direct bearing upon actions taken in other areas such as information security. When security policy functions are fragmented, the chances of inconsistent and ineffective protection levels are increased. Employees in security positions, whether it is security administrators, security chiefs, or security clerks, are critical to the national defense and deserve security policy that is clear, concise, and consistently applied to all echelons of security. In the absence of security policy that is streamlined, updated and harmonized, organizations will waste resources trying to comply with guidance that is potentially redundant, outdated and confusing.

Objectives

This is the third in a series of reports on security within the Department of Defense and is responsive to a request made by the Under Secretary of Defense for Intelligence (USD(I)) for the Office of Inspector General, Department of Defense, to assess the effectiveness of security in the Department. Specifically, we are conducting assessments of the following issue areas:

- how the Department programs and tracks its security costs and measures the return on investment for security expenditures;
- how security professionals are trained and certified/professionalized;
- how effective security policy is in addressing the security needs of the Department; and
- how security professionals' jobs are classified and graded.

This report addresses the effectiveness of security policy in addressing the security needs of the Department.

Scope and Methodology

This assessment was conducted in accordance with Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the assessment to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives.

Because of the size and complexity of addressing security within the Department of Defense, we are performing this assessment in phases: phase one, Tracking and Measuring Security Costs; phase two, Training, Certification, and Professionalization; phase three, Security Policy; and phase four, Classification and Grading. Subsequent reporting may also address security issues within a larger context as additional information is developed. To accomplish the objective, we reviewed relevant policies and guidance and interviewed officials responsible for security policy development and implementation.

Background

There have been previous assessments of security policies within the DoD. In 1985, “Keeping the Nation’s Secrets: A Report to the Secretary of Defense” was submitted to the Secretary of Defense by The Commission to Review Department of Defense Security Policy and Practices, headed by Richard G. Stilwell, General, USA (Retired). The report emphasized the need to respond to “the threat posed by hostile intelligence services by establishing a comprehensive set of policies and procedures designed to prevent unauthorized persons from gaining access to classified information.” The report also noted, however, that while protecting classified information was “imperative in principle” security policies were crafted in an environment of budgetary constraints and “tempered... by operational necessities.” The report further noted that some policies remained in force despite their proven ineffectiveness and concluded that “in the final analysis, safeguarding classified information comes down to proper supervision and the individual's responsibility to apply the rules.”

In 1994, The Joint Security Commission report entitled “Redefining Security,” addressed security policy and reported that security policy was fragmented. The report also identified the ad hoc manner in which security policies and practices have evolved noting that policy is enumerated in several documents prepared at different times, by different people in response to differing requirements and events – not as part of a comprehensive coordinated effort. The report further cited the disadvantages of developing policy through consensus noting that the approach is time consuming, ineffective, and results in inadequate policy that has been weakened in order to achieve consensus. According to the report, improvements in security policy could not be achieved without a unifying structure to provide leadership, focus, and direction.

A majority of the issues identified in the above reports remain true today. To date, DoD as a whole still needs to address the identified problems with security policies, including policy development and the approval process. In fact, these issues were also identified in a 2011 Office of the Under Secretary of Defense for Intelligence requested Federated Security study that assessed the optimal organizational, management, and resourcing structure to best accomplish the Department’s security mission. The study noted that “the existing organizational structure of the DoD security enterprise is fragmented with functions scattered across a number of organizations within DoD components. This results in a lack of central coordination and management of DoD security functions which include policy implementation and resourcing.”

Finding: DoD Needs an Overarching Security Policy to Advance an Integrated Enterprise Approach to Security

Within the DoD, security functions are disjointed. Moreover, in each security functional area, it is difficult - if not impossible - to manage security policy. While several security programs do exist within components, coordination is inconsistent at the Office of the Secretary of Defense level. As a result, DoD security components establish their own strategies, guidance, and reporting channels. This fragmented structure could result in ineffective application of protection across the Services and commands. The Department has taken steps to address the need for an integrated, coordinated, and comprehensive security framework through such measures as the creation of the Defense Security Enterprise Executive Committee (DSE ExCom), the Security Professional Education and Development (SPeD) program, and an overarching security policy that provides guidance for a comprehensive and integrated security framework - "Management of the Department of Defense Security Enterprise." However, DoD needs to promulgate the overarching policy in order to solidify the DSE ExCom and to strengthening security policy and enterprise management. This will significantly advance efforts to comprehensively integrated security guidance and ensure conformance with the developing enterprise paradigm within the Department.

DoD Enterprise Approach

As we have consistently stated, security is a critical function that spans the entire Department; and, as such, functional integration, governance, and strategic resource management can be better leveraged through an enterprise approach to security management. In responding to the recommendation in the first report in this series, the Deputy Under Secretary of Defense for Intelligence and Security stated that "Security policy administration within the Office of the Secretary of Defense is also fragmented. For example, information systems security comprises a significant portion of the costs incurred, but policy administration and oversight of this critical function are external to the Office of the Under Secretary of Defense for Intelligence. As a result, a process for decision-making and governance would have to be established to achieve the comprehensive security framework you recommend."

Current Enterprise efforts include DoD moving forward by creating an overarching security directive, DoD Directive 5200.LL, "Management of the Defense Security Enterprise," (Draft - with an anticipated publish date in fourth quarter FY 2012), consistent with the authorities assigned in DoD Directive, 5143.01, "Under Secretary of Defense for Intelligence (USD(I)," November 23, 2005, establishes policy and assigns responsibility for the management of the Defense Security Enterprise (DSE). It provides direction for a comprehensive DSE policy and oversight framework and governance structure to safeguard personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. It deconflicts the DSE from other DoD security related functions such as force protection and provides for the alignment, synchronization, support, and integration of those related security functions. It assigns responsibilities related to the DSE to the Defense Security Executive, and provides a common lexicon for the DSE.

It also established the DSE ExCom. The objective of the DSE ExCom is to provide enterprise-wide and converged organizational governance to the development, implementation, and oversight of security policy and security workforce development.

Members comprise senior leadership from key components in the Department who have corresponding oversight responsibility for security functions. The DSE ExCom represents a significant transformation in the way the Department is approaching security matters.

DoD 3305 series of issuances address the training, education, and professional development needs of the DoD Intelligence Enterprise. The series authorizes DoD functional managers and training councils to define workforce training standards. The training and professionalization of intelligence and security personnel is governed by these issuances. We addressed DoD Instruction 3305.13, “DoD Security Training,” December 18, 2007, in a previous report on security training, certification, and professionalization. The instruction resulted in the creation of the Defense Security Training Council. The training council provides the means through which security training issues, policy changes, establishment of standards, allocation of responsibilities, and other related topics can be addressed and recommendations made to the USD(I). The council incorporates a coordinated approach to security training and professionalization.

A major contributing factor to the training, education, and professional development efforts is the SPēD Program, which is a DoD-wide security training and certification program that will identify security proficiencies and accountabilities. When fully implemented by the fourth quarter of 2014, SPēD will provide the DoD security workforce a path towards professionalization and will establish standardized competencies across DoD components. Detailed information about the SPēD program can be found in our previous assessment¹ on security training, certification, and professionalization.

Current Security Policy

DoD components must be compliant with a number of security policies which can be redundant and outdated. Central oversight of security policies is only in its formative stages with the creation of the Defense Security Oversight and Assessment Program.² There is also no agreed upon lexicon for security, with the one exception being Information Assurance. The fragmentation and lack of top-down coordination of the security enterprise undermines the DoD mission and national security. The current organizational structure makes it difficult for any high-level decision-maker to know whether security functions are being adequately fulfilled. In effect, security policy is stove-piped, making it difficult to identify a senior level focal point for security programs.

DoD security policy is fragmented, redundant, and inconsistent; in part, because of the lack of an integrated security framework. The Department has a significant number of security policy publications, and specializations which cause redundancies, inconsistencies, and gaps in the creation and implementation of security measures. Currently, the Department has 23 security functional areas – each with its own set of

¹ “Assessment of Security Within the Department of Defense – Training, Certification, and Professionalization,” Report No. DoDIG-2012-001, October 6, 2011. This is the second report in the series of assessments.

² As part of its strategic oversight of security role in the DoD, on September 30, 2010, the OUSD(I) established the Defense Security Oversight and Assessment Program, with the primary purpose of gaining awareness of the health of the Defense Security Enterprise and making policy, planning, and advocate resourcing decisions necessary for continued improvement.

related security issuances. It is difficult to provide oversight and training associated in most security disciplines when there are no clearly defined responsibilities and lines of authority for information security, physical security, and information assurance when dealing with information protection.

Critical infrastructure protection, nuclear physical security, cybersecurity, supply chain risk management, insider threat, force protection, foreign disclosure, technology transfer, information assurance and other DoD functional areas should influence and be influenced by security policy and oversight – the core responsibility of the Principal Staff Assistant for Security. However, no formal mechanism exists to exercise executive-level leadership that incorporates and integrates the views of all of these functions into a cohesive departmental security program with comprehensive, non-duplicative, and mutually understood roles and responsibilities. In the absence of an overarching security policy that provides a means for organizational coordination, resulting policy can be stove piped, overlapping, and contradictory.

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs oversees Mission Assurance, Anti-Terrorism, Insider Threat, Cyber Security, Critical Infrastructure Protection, Force Protection, and Supply Chain Risk Management. The Under Secretary of Defense for Acquisition, Technology, and Logistics oversees nuclear physical security; the Under Secretary of Defense for Policy oversees foreign disclosure; and the DoD Chief Information Officer oversees information assurance.

These DoD functional areas should influence and be influenced by security policy and oversight – the core responsibility of the Principal Staff Assistant for Security. DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),", November 23, 2005, paragraph 4 states that "The USD(I) is the [Principal Staff Assistant] and advisor to the Secretary and Deputy Secretary of Defense regarding...security..." The USD(I) has the authority to develop and integrate risk-managed security and protection policies and programs; and develop, coordinate, and oversee the implementation of DoD security policies and programs.

The Deputy Under Secretary of Defense for Intelligence and Security, through the OUSD(I) Director of Security, has personnel who are responsible for maintaining the 43 policies promulgated by the office, covering the functional areas of information security, industrial security, operations security, research and technology protection, personnel security, physical security, and special access programs. However, no overarching policy exists that blends these policies into an integrated security framework for the Department.

Overlapping policies can not only be confusing, but there is a need to reduce potential duplication across federal programs, save tax dollars, and more efficiently use available resources. Accordingly, DoD security lines of authority and security policy should be revised to avoid redundancy and inconsistencies. A review of Information Security policy reveals overlaps between the following issuances:

- DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information," overlaps with personnel security matters by addressing persons authorized to access DoD unclassified controlled nuclear information and detailing how to obtain authorization to access the information. The issuance establishes access guidance for federal employees, contractors, congressional officials and other designated authorities. The issuance also identifies the appropriate process for marking unclassified controlled nuclear information and

thus overlaps with recent guidance for the appropriate handling and marking of controlled unclassified information as set forth in DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” February 24, 2012.

- DoD Instruction 5200.33, “Defense Courier Operations (DCO),” overlaps with physical security as it identifies standards for material storage for items in courier possession, escort requirements and material transit specifications. The issuance also overlaps with personnel security by identifying the security clearance and suitability standards for courier personnel.
- DoD Instruction 5200.39, “Critical Program Information Protection Within the Department of Defense,” overlaps with industrial security as it addresses the conduct of security inspections at cleared Defense contractor facilities as well as coordination with defense contractors. In addition, the instruction overlaps with matters related to operations security, personnel security, and physical security.

Additional review of physical security policy revealed the following policy overlaps.

- DoD Instruction 5100.76 “Safeguarding Conventional Arms, Ammunition, and Explosives (AA&E)” overlaps with physical security as it includes guidance for the proper safeguarding of Conventional AA&E against theft, loss, sabotage, damage, or unauthorized use. The instruction also addresses personnel security and foreign visits and assignments and overlaps with research and technology protection.
- DoD Instruction 5210.65, “Minimum Security Standards for Safeguarding Chemical Agents,” overlaps with industrial security with the provision of security standards for facilities that produce, store, use, train with, transfer, and/or destroy chemical agents. The instruction overlaps with personnel security by identifying standards for Individuals certified by Certifying Officials with a legitimate need to handle and/or use chemical agents. In addition, the requirement for a secure inventory database system and information protection measures to verify the appropriate security of information on chemical agents impinge on areas related to information security.
- DoD Regulation 5200.08-R, “Physical Security Program” prescribes minimum standards for the security of personnel, installations, military operations, and certain additional assets. As such, it overlaps with personnel security with respect to checks, issuance of clearances and identification cards; information security with respect to access to government systems and the coordination of physical security for automated information systems.

The above examples are not comprehensive. There are additional security policies with overlapping areas of control or guidance. These policies illustrate the integrated nature of security throughout the department and reflect the need for an enterprise approach in creating security policy.

Fragmentary security policies have been identified in previous DoD-sponsored studies. The earlier referenced Federated Security Study that assessed the optimal organizational, management, and resourcing structure to best accomplish the Department’s security mission identified the DoD Manual 5220.22-M, “National Industrial Security Program

Operating Manual,” as an issuance that does not reference requirements for Special Nuclear Material and does not cover operational data integrity and system availability, nor does it address controlled unclassified information. However, there is a draft 5220.22 manual that is undergoing formal coordination. These issues should be addressed in the revised version of the manual. An additional issuance, DoD Regulation 5200.2-R offers guidance for the safeguarding of personnel security investigative records but provides no direction regarding training of personnel tasked to safeguard records or the potential consequences for the deliberate or unintentional compromise of personnel security information.

Inconsistent security policies make it difficult for end-users to be in compliance with existing guidance. The following policies are potential examples where guidance needs to be congruent or harmonized.

- DTM 09-012, requires coordination with personnel security due to vetting and adjudication procedures of personnel receiving U.S. Government identification credentials. The two functions must work together to eliminate conflicting implementation guidance. It also has implications on industrial security for contractors and information security for network requirements.
- DTM 04-010, “Interim Information Security Guidance,” addresses a variety of issues, but does not assign specific responsibilities to specific organizations.
- DoD 5200.08-R, sets the stage for establishing common baseline physical security standards for all DoD Components, and then delegates implementation of that posture to each Component and its respective Component Head.

DoD Directive 5200.2, “Personnel Security Program,” was generally adequate with the exception of reciprocal acceptance of prior investigations and personnel security determinations. This is not uniform across the federal government. DoD has exceptions to certain types of investigations completed by other than DoD agencies. In the special access program area, DoD component Special Access Program Coordination Offices have documented agreements in place to accept no-waiver special access program eligibility determinations. There is still a challenge between the intelligence community and DoD in creating consistent standards for eligibility and reciprocity between sensitive compartmented information and DoD special access programs.

The personnel security requirements for individuals that require access to sensitive compartmented information are contained within Director of Central Intelligence Directive 6/4 and DoD 5105.21-M-1, “Department of Defense Sensitive Compartmented Information Administrative Security Manual,” August 1998; while the Joint Air Force, Army, Navy 6/4 manual provides the same requirements for the special access program community.

Department of Defense Instruction 5205.13, “Defense Industry Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities, January 29, 2010, does not address how DoD and the Defense Industrial Base will conjointly address certification and accreditation efforts of Defense Industrial Base systems, what standard to use, (e.g. the DoD Information Assurance Certification and Accreditation Process), and how this will be overseen.

Survey Results Regarding Security Policy

The above issues were also expressed in surveys that our office conducted in connection with this assessment. We solicited input from Security Managers via surveys in an attempt to ascertain the state of security policy across organizations, Services, and commands. Respondents were provided with a password to access the survey online. The survey was sent to 48 Security Managers throughout the DoD and addressed funding, certification and training, classification and grading, and policy issues related to security.

As the security managers of their respective organizations, respondents were able to provide knowledgeable responses and a perspective of security operations in the field where policy is implemented, which in turn informed this report. We received a response rate of 35%. Survey respondents noted that security policy is effective; however, one third of the Security Managers had inconsistent, overlapping, or difficult to implement policy.

A majority of survey respondents stated that they would like to see specific guidance directing the field and the central adjudication facilities to accept other organizations' adjudicative decisions, the reciprocal acceptance of prior investigations and personnel security determinations when processing new hires from the Services or when contractor personnel change to another contract or contracting company. With one overarching policy, personnel security delays in these cases could be eliminated and have the potential to save money for the Department.

More than one quarter of the survey respondents had serious concerns about the information security program, DoD Instruction 5200.01. Specifically, the concerns were absence of a consistent standard for marking classified information across the Department and whether the Information Security Oversight Office or Controlled Access Program Coordination Office guidance had primacy within the DoD. With one overarching policy, guidelines could be established to create one standard, regardless of agency, for marking, handling, transporting, or transmitting classified information.

An additional concern listed by survey respondents was the redundant policy within the physical security program, DoD Regulation 5200.08-R and the DoD antiterrorism/force protection program, DoD Directive 2000.12. For example, one survey respondent stated "I am constantly amazed at why we (the DoD) have separate physical security and antiterrorism programs. They are two sides of the same coin and are often duplicative and redundant."

Best Practice

The Air Force is making great strides in streamlining their security policies by undertaking efforts to consolidate security policy issuances. These efforts should be encouraged. The organization has unity of command over security functions by having a single senior executive reporting directly to the Secretary of the Air Force. The Administrative Assistant to the Secretary of the Air Force is the Senior Security Official and has established the Air Force Security Policy and Oversight Board comprising general officer and executive-level membership from across Air Force security and including key functions such as information assurance, legislative affairs, and others. As its name implies, the board decides on key initiatives and policy to be applied Air Force wide.

Air Force Policy Directive 16-14, "Information Protection," September 28, 2010, establishes policies and responsibilities for the oversight, management, and execution of protecting Air Force information across the Air Force Enterprise regardless of where the information exists. The Directive consolidates DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, and DoD Directive 8500.01E, "Information Assurance," April 23, 2007, and selected information protection policy from Air Force Policy Directive 10-7, "Information Operations;" Air Force Policy Directive 33-3, "Information Management;" Air Force Policy Directive 35-1, "Public Affairs Management;" Air Force Policy Directive 16-6, "Arms Control Agreement;" Air Force Policy Directive 61-2, "Management of Scientific and Technical Information;" and Air Force Policy Directive 63-1/Air Force Policy Directive 20-1, "Acquisition and Sustainment Life Cycle Management."

Conclusion

In the first report in this series, Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense: Tracking and Measuring Security Costs," August 6, 2010, we recommended a comprehensive and integrated security framework to facilitate tracking security costs, more accurately programming future years security budgets, and examine the return on investment for security expenditures.

We are not making any recommendations in this report because we believe that the previous recommendation, if implemented in a timely manner, will ensure an enterprise approach to security policy management across the Department. Further, our recommendations will ensure that the new DSE ExCom, with its inaugural meeting in January 2012, will be an integral part of policy development and coordination with the requisite authorities to effect changes in security policy implementation and oversight.

The DSE ExCom is furthering an enterprise-wide and converged organization perspective to security policy development, oversight, and implementation. The DSE ExCom will enable a unified Defense perspective on security issues across the DoD and provides a means to more effectively interface with external agencies and organizations. This integrated approach should be reflected in the existing security policy construct. At present, however, security policy is not in accordance with the DoD enterprise approach. Interviews, directed studies, and surveys have identified DoD security policy that is fragmented, redundant, and inconsistent.

An overarching security policy could lay the groundwork for an integrated framework for security policy implementation, provide an archetype for policy harmonization, and ensure greater security policy coordination and integration. DoD needs to promulgate the overarching policy in order to solidify the DSE ExCom and to strengthen security policy and enterprise management. This will significantly advance efforts to comprehensively integrate security guidance and ensure conformance with the developing enterprise paradigm within the Department.

APPENDIX: Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoDIG) have issued four reports that have addressed security specific to the DoD and national security enterprise. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov>. Unrestricted DoD IG reports can be accessed at <http://www.dodigmil/ir/reports>.

GAO

GAO Report No. GAO-09-0904SP, “Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing,” September 2009

DoD IG

DoD IG Report No. 10-Intel-09, “Assessment of Security Within the Department of Defense – Tracking and Measuring Security Costs,” August 6, 2010

DoD IG Report No. DoDIG-2012-001, “Assessment of Security Within the Department of Defense – Training, Certification, and Professionalization,” October 6, 2011

Office of the Under Secretary of Defense for Intelligence Comments



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

JUL 09 2012

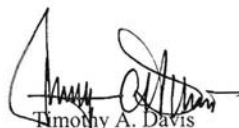
MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: MR. RAINEY, DEPUTY ASSISTANT INSPECTOR
GENERAL FOR INTELLIGENCE EVALUATIONS)

SUBJECT: Draft Report on the Assessment of Security Within the Department of Defense –
Security Policy (Project No. D2010-DINT01-0066.002)

The Security Directorate, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), concurs with the subject draft report. The information identified in this report is consistent with issues raised in prior Inspector General reports of this series. Therefore, no comments are submitted for inclusion in the final report.

With respect to progress made, OUSD(I) has implemented a comprehensive framework to enhance the Department's security posture, including: the activation of the Defense Security Enterprise Executive Committee (and supporting advisory group) for oversight and governance, and the imminent publication of our new security policy issuance, DoD Directive 5200.LL, "Management of the Department of Defense Security Enterprise." With its issuance this month, security policy will evolve and adapt to properly align, synchronize, and integrate security functions. Furthermore, these refinements will all be orchestrated under the supervision of an informed governance body. Security Directorate believes the implementation of these measures will sufficiently address and resolve the issues mentioned in this report.

The efforts of your team are appreciated by all in this directorate and contribute to our pursuit of generating relevant and effective security policy for the Department and our partners in industry.



Timothy A. Davis
Director of Security





Inspector General Department of Defense

